

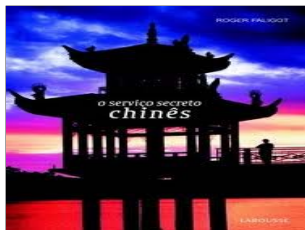


Brasília-DF, 25 de Agosto de 2010 - 22h59

Opinião

Ascensão e queda dos Serviços Secretos e a China

25/08/2010 - 15h56



Bernardo Wahl Gonçalves de Araújo Jorge

Em 19 de janeiro de 2010, foi assassinado, em Dubai (Emirados Árabes Unidos), um importante líder da organização palestina Hamas: Mahmoud al-Mabhouh.

A equipe responsável pela morte de Mabhouh não conseguiu conduzir a operação em completo anonimato: é impossível operar em um ambiente moderno sem deixar nenhuma pista eletrônica.

A polícia de Dubai usou as imagens de equipamento de monitoramento de vídeo do aeroporto, hotéis e de um *shopping center* próximo ao local do ocorrido para traçar os movimentos dos operativos e definir suas identidades, conforme os passaportes que usaram.

Eram passaportes muito bem falsificados do Reino Unido, Irlanda, Alemanha e França.

Os cartões de crédito usados pelos operativos, aliás, estavam ligados a uma empresa chamada Payonner, cujo *CEO* (*Chief-Executive-Officer*) é um antigo membro das Forças Especiais das Forças de Defesa Israelenses (IDF, na sigla em inglês).

A descoberta dos passaportes fraudulentos criou um problema diplomático para Israel, considerando que o *Mossad* estava no topo da lista dos suspeitos.

A questão é que muitos detalhes da operação vieram à tona, colocando em perigo o anonimato que deve cercar este tipo de operação.

Outro episódio, ocorrido em junho do mesmo ano, nos Estados Unidos, também despertou nossa atenção.

Após a visita do presidente russo, Dmitri Medvedev, o FBI (*Federal Bureau of Invesatigations*) prendeu, em Arlington (Virgínia), dez “ilegais” suspeitos de espionarem para a Rússia, mais especificamente de agirem para o SVR (o Serviço de Inteligência Estrangeira russo).

A missão destes operativos era se infiltrar em círculos de poder dos Estados Unidos para tentar recrutar pessoas do alto escalão, as quais forneceriam informações para o centro em Moscou.

Para a Rússia, segundo alguns analistas, mais vale investir em espionagem do que em pesquisa e desenvolvimento.

Análises preliminares entenderam que, mesmo após vinte anos após o fim da Guerra Fria, o chamado “grande jogo” continua entre Moscou e Washington, e a Rússia ainda usa a coleta de inteligência como uma ferramenta fundamental de sua política externa.

Os Estados Unidos ainda são vistos com desconfiança por parte dos russos.

Não é à toa: a intromissão em assuntos dos Balcãs, a expansão da OTAN (Organização do Tratado do Atlântico Norte) para o leste europeu, a criação de um sistema de defesa anti-mísseis na Polônia e na República Checa e o envolvimento de Washington nas crises da Geórgia, da Ucrânia e na Ásia Central, não agradaram a Rússia.

Operações deste tipo geralmente demoram muitos anos.

Para os russos é interessante viver infiltrados nos EUA, considerando a qualidade de vida.

Porém, para os norte-americanos, não é interessante viverem infiltrados em outras culturas.

Dessa forma, grande parte da inteligência estadunidense vem do monitoramento de comunicações (a chamada inteligência de sinais), principalmente através da NSA (*National Security Agency*), embora existam muitas outras agências (cerca de 16, sem contar todo o aparato privado revelado recentemente por reportagem do *The Washington Post*).

O que este episódio envolvendo operativos russos mostrou é que os “antigos métodos” ainda sobrevivem mesmo em um contexto no qual as ameaças avançam para o espaço informacional, ou ciberespaço.

E é aí que surge a questão China.

Pela primeira vez, segundo reportagem do *The Boston Globe*, o Pentágono tornou público um aviso sobre o uso, por parte do Exército Popular da China (PLA, na sigla em inglês), de especialistas civis em computação para conduzirem ataques cibernéticos clandestinos direcionados à agências do governo norte-americano e à empresas

dos EUA.

Trata-se de “unidades de guerra informacional” que desenvolvem vírus para atacarem sistemas e redes de computadores, sendo que tais unidades envolvem profissionais de computação civis (ou “mercenários cibernéticos civis”, conforme o *The Boston Globe*).

E é uma ferramenta que será amplamente usada pela China: as novas tecnologias, conforme mostrado pelo jornalista Roger Faligot no robusto livro *O Serviço Secreto Chinês*, da editora Larousse (2010).

Trata-se de uma leitura bastante densa, cheia de dados e informações, entre elas de que um sinal incontestável de abertura da China é que “livros históricos sobre a inteligência chinesa podem ser comprados em Pequim, na livraria das Edições do Exército Popular de Libertação, ou em qualquer banca da capital” (p. 142).

Enquanto o Mossad e o SVR “expõem” seus agentes, a China navega nos meandros e nas sombras da Sociedade em Rede, seguindo sua “ascensão pacífica”.

Referências

BALDOR, Lolita C. “Pentagon Warns Public About Cyber Attacks by China”. *The Boston Globe*, August 20, 2010. Notícia produzida originalmente pela *The Associated Press*.

BURTON, Fred; WEST, Ben. “Using Intelligence from the al-Mabhouh Hit”. *Stratfor Global Intelligence*, March 3, 2010.

FALIGOT, Roger. *O Serviço Secreto Chinês*. São Paulo: Larousse do Brasil, 2010.

MCGREAL, Chris. “FBI breaks up alleged Russian spy ring in deep cover”. *The Guardian*, June 29, 2010.

MONIQUET, Claude. Briefing: First Lessons from the Affair of the Russians ‘Ilegals’ in the United States. *European Strategic Intelligence and Security Center*, 29 jun. 2010.

Bernardo Wahl Gonçalves de Araújo Jorge é professor Mestre em Relações Internacionais (FMU-SP). E-mail: bernardowahl@gmail.com

"É permitida a reprodução total ou parcial, desde que citada a fonte"

Fonte: www.inforel.org